


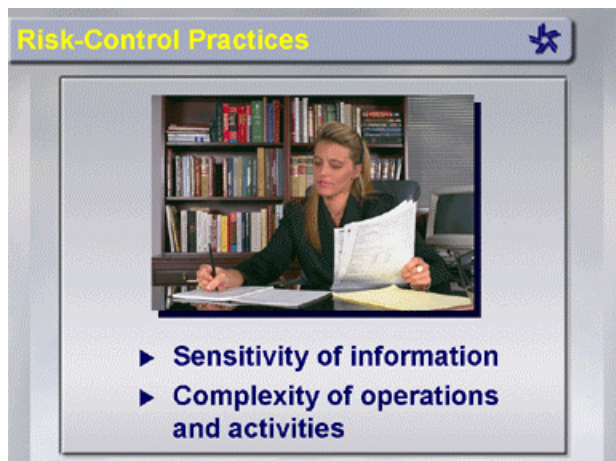
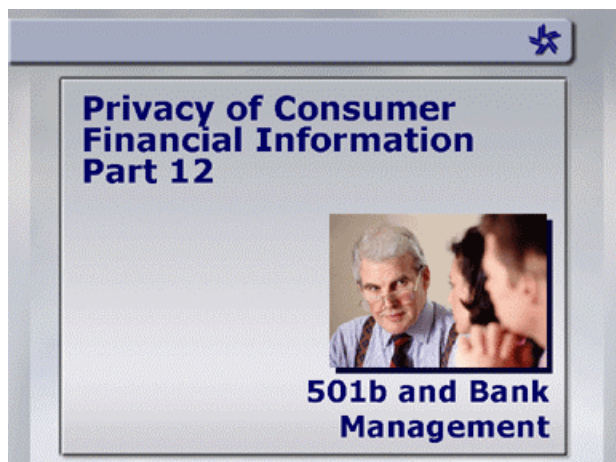
PRIVACY OF CONSUMERS' FINANCIAL INFORMATION PART 12 501(b) AND BANK MANAGEMENT

RESOURCES PROVIDED THROUGH

FFIEC InfoBase 

APRIL 2001

Slides



Narration

In the last presentation, you learned about some of the general responsibilities that a bank's board and management should assume in order to protect their customer's nonpublic, personal information. This presentation will take a more detailed look at what 501(b) guidelines require of bank management.

We'll discuss guideline requirements for risk-control practices, training and testing issues, monitoring risk-control plans, and, finally, reporting requirements.

Management can best control risk by establishing written policies and procedures—policies and procedures that are commensurate with the sensitivity of the information being protected and the complexity and scope of the bank's operations and activities.

Risk-Control Issues



During your examinations, keep in mind that assessment of the effectiveness of an institution's risk-control practices includes issues like:

Risk-Control Issues

- ▶ Access to data
- ▶ Physical access to locations
- ▶ Encryption process
- ▶ Change control procedures
- ▶ Operational policies

- Access to data (including practices such as authentication requirements and access control procedures)
- Access to physical locations (such as buildings, computer rooms, and record storage facilities)
- Encryption of electronic customer information (while it is in transit or in storage)
- Change control procedures (such as protocols for updating software programs)
- Operational policies (such as dual control procedures, segregation of duties, and employee background checks)

Disaster Recovery

Protecting consumer's nonpublic personal information from:



- ▶ Fire
- ▶ Water damage
- ▶ Technical failures

An especially integral part of a bank's risk control practices is its disaster-recovery plan. Examiners should consider this as an important element when evaluating a bank's overall risk control efforts.

Ask yourself if plans are in place for recovering information that could be lost to natural or environmental hazards such as the ones listed here.

Management Responsibilities

- ▶ Risk-control practices
- ▶ Training and testing issues
- ▶ Monitoring risk-control plans
- ▶ Reporting requirements

Effective risk control requires a bank to do more than just develop a set of static plans.

Once the plans are in effect, banks should also have ongoing training, testing, and monitoring programs built into their processes.

Security plans are only as effective as the bank staff's ability to implement them.

Training



- ▶ Actions
- ▶ Responsibilities
- ▶ Critical staff

Consequently, banks should also have a comprehensive security training plan in place.

The training should clearly define not only what actions should be taken, but also who should take those actions and who should be informed of possible security breaches as they arise.

Testing



Likewise, management needs to have a regularly scheduled testing program in place. This program should be similar to what regulatory agencies expect for disaster recovery plan testing.

Once in place, security plans should be tested to ensure that the institution knows that the plan will actually do what it was intended to do.

Bank-Specific Testing

Based on:

- ▶ Risk-assessment results
- ▶ Changes in internal and external conditions

The frequency and nature of the testing should be evaluated based on the results of the institution's risk assessment, and the testing should be coordinated with changes in internal and external conditions that might affect information security.

Testing Plans

...should reflect changes in internal and external conditions.



For example, testing should take into account changes in staff, systems, procedures, or vendors.

Testing Process

- ▶ Testing conducted by independent third parties
- ▶ Results reviewed by independent third parties



Testing should be conducted and reviewed by independent third parties. These individuals can be either internal personnel or external consultants, as long as they're not directly involved with information security at the institution. Of course, they must also have the expertise required to conduct the testing and to evaluate the results.

Management Responsibilities

- ▶ Risk-control practices
- ▶ Training and testing issues
- ▶ **Monitoring risk-control plans**
- ▶ Reporting requirements

Bank management also needs to monitor their information security program continually.

Monitoring Information Security

- ▶ **Technology**
- ▶ **Sensitivity of customer information**
- ▶ Internal or external threats
- ▶ Bank business arrangements

The monitoring should reflect changes to the bank's technology, the sensitivity of customer information, internal or external threats, and the bank's business arrangements, such as mergers, acquisitions, alliances, and so forth.

Risk Monitoring

- ▶ **Monitoring systems to detect possible compromise to information**
- ▶ **Response program to handle attacks on information security**



Management should not only have monitoring systems in place to detect possible compromise of customers' non-public, personal information, but they should also have an established and tested response program in place for handling specific intrusions.

It's important that banks have these monitoring and response systems well thought out and documented in advance of any actual threat to the security of customer information.

Management Responsibilities

- ▶ Risk-control practices
- ▶ Training and testing issues
- ▶ Monitoring risk-control plans
- ▶ Reporting requirements

Finally, the guidelines establish requirements for management to report the status of information security programs to the board, or an appropriate board subcommittee, on at least an annual basis.

Reporting Requirements

- ▶ Overall status
- ▶ Bank compliance



The reports should discuss the overall status of the information security program and the bank's compliance with 501(b) guidelines.

Reporting Requirements

- ▶ Overall status
- ▶ Bank compliance
- ▶ Additional Information
 - ▶ Risk-assessment practices
 - ▶ Risk-management and control decisions
 - ▶ Outsourcing
 - ▶ Test results
 - ▶ Security breaches and responses
 - ▶ Recommendations for change

The reports should also discuss, as appropriate, risk-assessment practices, risk-management and control decisions, outsourcing, test results, any security breaches (and management's response to them), and recommendations for change.

Outsourcing

The bank is still responsible for :



- ▶ Protecting consumer information
- ▶ Exercising due diligence
- ▶ Requiring that guidelines are met

One last thought, which really applies to all of the management responsibilities we've discussed, is that of outsourcing.

Bank management must exercise due diligence in managing and monitoring outsourcing arrangements, and require (by contract) that vendors implement appropriate measures to meet the objectives of the privacy guidelines.

Vendor Monitoring



Institutions maintain responsibility for protecting their customers' nonpublic personal information.

The critical point to keep in mind is—a bank's choice to outsource services does not mean that it can abdicate its responsibility to properly protect its customers' nonpublic personal information.

Vendor Monitoring

You can view additional information on vendor monitoring by opening the document *Risk Management of Outsourced Technology Services* from the menu on the right side of your screen.

Vendor Monitoring

- ▶ Internal audits
- ▶ Independent audits
- ▶ Information security plans
- ▶ Organizational procedures
- ▶ Test results

Monitoring should include review of items such as the outsourcing vendor's internal and independent audits, information security plans, organizational procedures, and test results. Again, these activities should be commensurate with the risk the bank has and the criticality of the information.

Management Responsibilities

- ▶ Risk-control practices
- ▶ Training and testing issues
- ▶ Monitoring risk-control plans
- ▶ Reporting requirements

In this presentation, we've looked at some of the primary management responsibilities that you should consider when you review a bank's compliance to 501(b) guidelines.

This information, and that in the earlier 501(b) presentation, will help as you begin to add the protection of customers' nonpublic personal information to your examination activities.